| NODIS Library | Organization and Administration(1000s) | Search |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |
| NODIS Library | Organization and Administration(1000s) | Search |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2009

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 1 (11/08/2005)

Responsible Office: Office of Security and Program Protection

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 2: NASA PERSONNEL SECURITY PROGRAM: REQUIREMENTS , INVESTIGATIONS , AND ADJUDICATION PROCESS FOR POSITIONS (NATIONAL SECURITY POSITIONS) REQUIRING ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI)

2.1 General

2.1.1. Title 5 Code of Federal Regulations (CFR), Part 732, National Security Positions, requires each agency to follow established procedures to identify national security positions. Positions identified by this process within the National Aeronautics and Space Administration (NASA) require regular use of or access to classified information. This chapter addresses the sensitivity designation program associated only with national security, the criteria for determining national security sensitivity levels, and screening (i.e., the type of investigation) required under Executive Order (E.O.) 10450, Security Requirements for Government Employment, and E.O. 12968, Access to Classified Information.

2.1.2. This chapter does not address other aspects of the position risk designation program which include Personnel Suitability described in Title 5 CFR, OPM Part 731, Suitability; HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors , and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors," Automated Information System Security defined in the Office of Management and Budget (OMB) Circular A-130; and numerous laws.

a. These programs, outlined in chapters 3 and 4 respectively, require a determination of a position's risk level (i.e., Low Risk, Moderate Risk, or High Risk) using criteria that are separate and distinct from the national security criteria. Designation of position risk level must occur prior to establishment of sensitivity level. See Appendix M.

b. Information regarding Personnel Suitability may be obtained from the Office of Human Resources.

c. NPR 2810.10, NASA Automated Information Systems Security, establishes the policy, assigns responsibilities, and prescribes standards and procedures for the management of the Information Technology (IT) security program for NASA

2.1.3. Position sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a national security position, could cause to the national security.

2.1.4. Investigations are conducted to provide a basis for ensuring that the granting of a security clearance to an individual is clearly consistent with the interests of national security.

2.1.5. Personnel security reports and records shall be handled in accordance with the Privacy Act of 1974.

2.1.6. The Office of Personnel Management (OPM) conducts a range of investigations that satisfy the various requirements for the three position-sensitivity levels described in this chapter, as they relate to accessing CNSI.

2.1.7. NASA Contracts requiring the generation of and/or access to CNSI will be processed and individuals investigated in accordance with the requirements established in chapter 6 of this NPR, and the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

2.2 Scope

2.2.1. This chapter prescribes the procedures whereby employees are selected, processed, investigated, and adjudicated for national security positions, consistent with U.S. Security Policy Board (SPB) Procedures contained in SPB Issuance 1-97, SPB Issuance 2-97, and SPB Issuance 3-97.

2.2.2. This chapter does not apply to contractor personnel providing services under a NASA classified contract that requires access to CNSI. Refer to chapter 6, "Industrial Security," for requirements on NASA classified contract processes and procedures.

2.3 Responsibilities

2.3.1. The DSMD shall establish a Central Adjudication Facility (CAF) at the Headquarters level responsible for adjudicating all investigative results for security clearances for access to CNSI. The CAF shall process and manage all requests for security clearance, adjudicate all investigative results, grant clearance eligibility, and deny, revoke, or suspend security clearances in accordance with the provisions of EO 12968 due process considerations.

2.3.2. Center Directors shall ensure the CCS manages the Center personnel security program in accordance with this NPR.

2.3.3. The CCS shall:

2.3.3.1. Process security clearances for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

2.3.3.2. Ensure only the on-line e-QIP version of the SF 86 is used when it becomes available.

2.3.3.3. Grant a NASA employee a security clearance or suspend an employee's clearance for cause.

2.3.3.4. Delegate these responsibilities to a senior personnel security specialist who is a civil service employee, who has attended a recognized Personnel Security Suitability and Security Adjudication course, and who has maintained currency in that field.

2.3.3.5. In cooperation with Center Human Resources Organizations, management, and

supervisory personnel, implement these procedures for appropriate designation of National Security position sensitivity, per section 2.7, for all existing and newly established positions whose duties clearly reflect the requirement for a security clearance and access to CNSI, in accordance with the requirements set forth in this chapter. This collaborative approach is essential if NASA is to effectively comply with established national security position sensitivity designation requirements outlined in 5 CFR 732.101 - 732.401 and the requirements of EO 12968.

2.3.4. Center Human Resources Organizations shall:

2.3.4.1. Ensure that position descriptions are developed by the appropriate management and supervisory personnel, and that they accurately reflect National Security position sensitivity and establishes clear requirements for access to CNSI, as required under 5 CFR 732.101 - 732.401 and EO 12968.

2.3.4.2. Ensure no recruitment, hiring, or change of position action takes place until the appropriate position sensitivity level and risk designation has been established.

2.3.4.3. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this chapter.

2.3.5. Program, line managers, and supervisors shall ensure full compliance with the requirements established in this chapter.

2.4 Personnel Security Program Oversight

As part of its responsibility for the functional management of the NASA Security Program, the DSMD shall include personnel security program matters in periodic audits of Center security programs.

2.5 Basic Principles of Personnel Security Clearance Management

2.5.1. EO 12958, Classified National Security Information, clearly emphasizes the requirement to establish procedures to prevent unnecessary access to classified information, including procedures that require that a demonstrable need for access to classified information be established. EO 12968, Access to Classified Information, directs that when such access is no longer required, it shall be administratively withdrawn.

2.5.2. Due to the cost and time invested in conducting the appropriate investigation, managers and supervisors must be judicious and accurate in determining an employee's need to access CNSI. Following the requirements established in Appendix M of this NPR, managers and supervisors must establish the access requirement during the development of the individual position description and assign the appropriate designation of position risk and sensitivity and risk level designation for each NASA position description. Failure to properly identify the need for access to CNSI upfront causes added expense that must be borne by the program and results in unnecessary delays for the Agency as it must then change or cancel previously submitted investigative requests with OPM.

2.5.3. No individual is deemed eligible for access to CNSI merely by reason of right or privilege or as a result of any particular title, grade, position, or affiliation.

2.5.4. Access to CNSI shall not be requested or granted solely to permit entry to, or

ease of movement within, NASA controlled areas when the individual involved has no need for access to classified information, and such access may be reasonably prevented.

2.5.5. Requests for security clearances shall not be processed or granted based merely on a speculative need for access. Requesting security clearances for contingency purposes in excess of actual official requirements is prohibited.

2.5.6. The level at which access to CNSI is requested and granted shall be limited and shall relate directly to the level of classified information to which access is clearly justified in the performance of official duties.

2.6 Processing Personnel Security Clearance Requests

2.6.1. As stated in subparagraph 2.5.2, the requirement for access to CNSI shall be clearly established during the position development phase. Once the position has been determined to require access to CNSI and position sensitivity assigned, the Center HRO shall ensure the new appointee receives access to and completes the on-line (e-QIP) SF 86 per section 2.7.

2.6.2. If an incumbent employee has been determined to require a security clearance up to the Top Secret level, a NASA Form 1630, Request for Access to CNSI, shall be prepared and appropriately justified by the employee's immediate supervisor, reviewed by the line supervisor through the Division Director, or higher depending on the applicant's organizational position, and forwarded to the Center Personnel Security Office for appropriate action.

2.6.2.1. The NASA Form 1630 shall be retained in local personnel security files, with a copy forwarded to the CAF.

2.6.2.2. A recertification (New NASA Form 1630) must be conducted only when a person changes position. However, annual review of clearance and access requirements is necessary to ensure Center personnel security clearance needs are properly managed. The CCS will develop and implement the appropriate local procedures necessary to ensure a viable review is conducted.

a. Personnel with clearances who have not had the need to access CNSI during the previous year will be given serious consideration for administrative withdrawal of their clearance.
b. Clearances will not be retained merely as a stop-gap measure in the event the holder may need access to CNSI. There must be a clear demonstrable operational requirement to possess the clearance.

2.6.3. All required investigative forms shall be completed in a timely manner, by the employee and submitted to the CCS for appropriate action. Completion of electronic web-based investigative forms (e-QIP) shall be made mandatory as they become available online. (NOTE: Failure to complete the necessary forms in a timely manner will result in a significant delay in initiating the appropriate investigation and granting of an Interim clearance up to and including the SECRET level.)

2.6.4. The CCS shall ensure the forms are properly completed and submitted to OPM for investigation using the NASA Central Adjudication Facility (NASA CAF) Security Office

Identifier (SOI) number provided by the NASA CAF. [NOTE: Use of the NASA CAF SOI number will ensure completed investigations are returned by OPM to the Central Adjudication Facility (NASA CAF) for adjudication.]

2.6.5. Results of the adjudication process shall be posted and made available to Center security offices via the Clearance Verification System (CVS) Database. The NASA CAF shall notify Center security offices when information on processed employees has been entered into the CVS. The CCS may then grant final clearance. The employee will be notified, in writing, when an Interim or Final clearance has been granted. Use of NASA Form (NF) 1730, "Obtaining and Maintaining a Security Clearance for Access to Classified National Security Information (CNSI)," is mandatory for communicating clearance status and requirements to employees.

2.6.6. Requests for Sensitive Compartmented Information (SCI) access requires the submittal of Form 2018A, (Special Access Request).

2.6.6.1. Personnel Requesting SCI access must have a completed TS investigation.

2.6.6.2. The Form 2018A must be prepared and justified by the employee's immediate supervisor. The line supervisor through the Division Director, or higher depending on the applicant's organizational position, shall also review and approve the submittal, and forward it, along with copies of the employee's personnel security file (PSF) and an additional copy of an updated SF 86, to the HQ Special Security Office (SSO) for appropriate action.

2.6.6.3. The Form 2018A and the original signed SCI Non-disclosure Form shall be retained by the SSO representative at the Center. A copy of the signed SCI Non-disclosure Form shall be forwarded to the NASA HQ SSO.

2.6.7. One-Time Access Determinations

2.6.7.1. Occasionally, urgent operational requirements may occur where NASA civil service personnel employees in nonsensitive positions with no security clearance eligibility determination have a one-time or short duration requirement for access to CNSI at the Confidential or Secret level or are required to possess a Secret clearance to access other Government agency secure sites even though the purpose for their visit is of an unclassified nature. Usually, the limited duration or nature of this access requirement does not warrant processing the individual for a personnel security investigation and final security clearance eligibility determination. One-time access determinations shall not be granted for the Top Secret level. One-time access determinations shall be used sparingly and only under conditions of compelling government need. The CCS has the authority to grant one-time access determinations subject to the following terms and conditions:

a. One-time access determinations shall not be issued more than 3 times per person and shall not exceed 60 days in total accumulated duration during a single calendar year.

b. One-time access determinations shall only be granted to U.S. citizen civil service personnel that have been continuously employed by the Federal Government for the preceding 24 months.

c. Whenever possible, access shall be limited to a single instance or only a few occasions. Repeated access requests shall require processing for final security clearance determination.

d. If the need for access is expected to exceed the original request of 60 days, the individual must be processed for a final security clearance determination.

e. An individual requiring one-time access must complete a NASA Form 1630, Request for Access to CNSI; have a prior completed "no access" National Agency Check or other comparable personnel security investigation, or a criminal history and credit check, a favorable suitability determination and local records check; present a completed SF 86 or 86C, if applicable; and be personally interviewed by the CCS or qualified designee.

f. One-time access determinations and subsequent debriefs shall be documented in local files and any security clearance certification (i.e., one-time clearance granted from date-to-date) properly recorded.

2.7 Coding of Position Sensitivity Level Designations for National Security Positions

2.7.1. The proper coding of position sensitivity for national security positions is required on Optional Form 8, Position Description, or NASA Form 692, Position Description, and optional on the SF 50 and 52. (See 5 CFR part 732). NASA managers and supervisors must use the following codes whenever establishing position sensitivity for access to CNSI: National Security Position Sensitivity Level Codes:

Special-Sensitive: 4
Critical-Sensitive: 3
Noncritical-Sensitive: 2
Non-Sensitive: 1 (No clearance required).

2.7.2. Center Human Resources Offices are responsible for managing a Risk Designation System in accordance with 5 CFR 731-106(a). They shall coordinate, in a timely manner, with managers, supervisors, and the CCS to accomplish sensitivity designation of positions requiring access to CNSI. After the appropriate position sensitivity determination has been assigned, the Center HRO or Security Office shall initiate the appropriate investigation.

2.7.2.1. SPECIAL-SENSITIVE (SS): Positions requiring access to any of the levels of classified information outlined below shall be designated Special-Sensitive. Individuals in or selected for these positions must undergo a Single Scope Background Investigation (SSBI), using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access to:

a. Top Secret SCI

b. NASA Special Access Program

2.7.2.2. CRITICAL-SENSITIVE (CS): Positions requiring access to any of the levels of classified information outlined below shall be designated Critical-Sensitive. Individuals in or selected for these positions must undergo a Single Scope Background Investigation (SSBI), using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access to:

a. Top Secret (TS)

b. NATO Top Secret

2.7.2.3. NONCRITICAL-SENSITIVE (NCS): Positions requiring access to any of the levels of classified information outlined below shall be designated Noncritical-Sensitive. Individuals in or selected for these positions must undergo, at a minimum, an Access National Agency Check with Inquiries (ANACI), using Standard Form 86 (SF-86), and be favorably adjudicated prior to being granted access. Exceptions to classified access investigative requirements for these positions shall be made only as provided for in section 2.6 above.

a. a. Secret or Confidential

b. b. NATO Secret/Confidential

2.7.2.4. Pre-appointment investigation requirements shall NOT be waived for positions designated "SPECIAL SENSITIVE."

2.7.2.5. Pre-appointment waivers may be authorized by Center Directors and the Assistant Administrator for Security and Program Protection to approve an emergency appointment or reassignment to a "CRITICAL SENSITIVE" or "NONCRITICAL SENSITIVE" position prior to completion of the required pre-appointment investigation only when clear justification exists to warrant the waiver.

2.7.2.6. Non-SENSITIVE: Non-sensitive positions relate to any position that is not a "National Security Position."

2.7.3. All NASA national security position descriptions (PD) shall be "Testing Designation Positions (TDP)." Personnel holding active clearances shall be entered into the Agency's random drug testing program.

2.8 Temporary/Interim Access to CNSI

2.8.1. Senior Management Officials shall request temporary access eligibility for U.S. citizen employees, civil service employees, contractors, and/or consultants filling CS and NCS positions when essential operational requirements do not allow for waiting for a pending personnel security investigation to be completed and adjudicated. Management shall submit requests for temporary access eligibility using NASA Form 1630 and provide compelling justification to warrant access to CNSI in advance of formal investigation and adjudication. The CCS shall serve as the appropriate adjudication authority and shall issue temporary access eligibility and grant the appropriate interim security clearance up to the Secret Level only, provided the provisions of SPB Issuance 3-97 (See Appendix C) are met. In all cases, the required personnel security investigation shall be initiated prior to issuance of the INTERIM clearance. Temporary/interim access eligibility and issuance of an INTERIM security clearance shall be recorded on NASA Form 346, Notification of Completion of Investigation, under Executive Order 10450. A copy of the NASA Form 346 shall be forwarded to the DSMD and local Office of Human Resources for inclusion in the subject's Official Personnel File (OPF).

2.9 Access to CNSI by Non-U.S. Citizens

2.9.1. Non-U.S. citizens (including lawful permanent resident (LPR)) are not eligible for a

security clearance. Under specific situations the AA/OSPP may authorize the granting of a Limited Access Authorization (LAA) to a non-U.S. citizen for specific information up to the Secret level when it has been determined that no U.S. citizen has the skills necessary to perform the work. The requesting organization shall submit a written request to the AA/OSPP via the CCS. The request shall:

2.9.1.1. Specify why it is impractical or unreasonable to use U.S. Citizens to perform the required work or function.

2.9.1.2. Define the individual's special expertise.

2.9.1.3. Define the compelling reasons for the request.

2.9.1.4. Explain how access shall be limited and physical custody of CNSI precluded.

2.9.1.5. The CCS shall review the request for accuracy, endorse or nonendorse it, and forward it to the AA/OSPP.

2.9.1.6. The AA/OSPP shall coordinate with the Office of External Affairs for concurrence (Export Compliance), and if approved, shall return it to the requestor. A copy shall be retained in the OSPP and CCS files.

2.9.1.7. A completed investigation and favorable adjudication are required before access is granted. The granting of Interim or Temporary access pending the completion of an investigation is prohibited.

2.9.1.8. Denied requests shall be returned to the requestor with an explanation of the denial.

2.9.1.9. Individuals with LAAs shall be placed under closely controlled supervision of appropriately cleared persons (U.S. Citizens). Managers shall be made aware of access limits imposed on these individuals and shall ensure compliance with any restrictions imposed.

2.9.1.10. Individuals who have been granted an LAA shall not be allowed access to any classified information other than that specifically authorized under national disclosure policy. Additionally, physical custody of classified information by these individuals is not authorized.

2.9.1.11. Non-U.S. citizens are ineligible for access to intelligence information, communications security keying materials, Top Secret information, Restricted or Formerly Restricted Data, Critical Nuclear Weapons Design Information (CNWDI), TEMPEST information, classified cryptographic information, or NATO classified information.

2.9.1.12. Classified access shall be limited to that necessary to complete the task, and access shall be terminated upon completion of the task.

2.9.1.13. Requests for access to CNSI owned by another agency must be coordinated with and approved by that agency.

2.9.2. If the access request is initiated by a NASA-cleared contractor performing on a NASA classified contract, only the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio, or successor organization, has the authority to grant an LAA to non-U.S. citizens. Procedures for coordination of the request are as follows:

2.9.2.1. A cleared contractor's Facility Security Officer must receive the endorsement of the CCS, Center International Visitor Coordina , tor (IVC), Center Export Administrator (CEA), AA/OSPP, and Office of External Relations (Export Control), as appropriate.

2.9.2.2. The CCS must ensure the contract is current and must evaluate the justification for the request. The non-U.S. citizen nominated for the LAA must prepare and sign a nondisclosure statement. The CCS shall forward the completed package to the AA/OSPP for review, coordination, and endorsement.

2.9.2.3. If acceptable, the AA/OSPP shall endorse and return it to the contractor for forwarding to the DISCO. A completed SSBI and favorable adjudication are required before access is granted.

2.9.2.4. Denied requests shall be returned to the contractor with an explanation of the denial.

2.9.2.5. Controls outlined in subparagraphs 2.9.1.9 through 2.9.1.12 shall be implemented and strictly monitored.

2.10 Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations from Other Government Agencies and Organizations

2.10.1. Reciprocity is a key component of current Federal personnel security philosophy, rules, and guidelines. NASA shall accept personnel security investigations and favorable determinations for access to CNSI conducted and adjudicated by other Federal agencies in accordance with the guidelines set forth herein.

2.10.2. Normally, prior investigations conducted in connection with actual or contemplated prior Federal service (civilian or military), the granting of a clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC) for access to Restricted Data (RD) or Formerly Restricted Data (FRD), or the granting of a security clearance under the Department of Defense (DoD) National Industrial Security Program (NISP), shall be accepted as meeting the investigative requirements prescribed herein, provided the following conditions are met:

2.10.2.1. There has been no break in service in excess of 24 months, and the prior investigation was completed within the timeframe established by SPB Issuance 1-97 for the level of access required.

2.10.2.2. The prior investigation meets the required scope and coverage standards and is compatible with the sensitivity of the position.

2.10.2.3. The prior investigation discloses no unresolved information that reflects adversely on the applicant's eligibility for a security clearance. If it is determined that prior investigation does not meet the provisions of paragraph 2.10.2 above, an appropriate update or upgrade investigation shall be requested to bring the total combined investigative effort up to standard.

2.11 Prior Personnel Security Clearance Determinations by NASA Authorities

Personnel security clearance eligibility granted by the NASA CAF and security

clearances granted by the respective NASA Centers shall be mutually and reciprocally accepted by all Centers without requiring additional investigation, unless there has been a break in the individual's employment in excess of 24 months or unless derogatory information that occurred subsequent to the last security determination becomes known.

2.12 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)

2.12.1. Access to Restricted Data (RD) and Formerly Restricted Data (FRD) outside the scope of aeronautical and space activities requires clearance by the Department Of Energy (DOE) or the Nuclear Regulatory Commission (NRC).

2.12.2. If such access is required solely for the performance of service for another agency, that agency normally shall initiate the required investigation. In such a case, the OPM reimbursable investigation required for the occupant of a sensitive position must not be initiated.

2.12.3. The Central Adjudication Facility (NASA CAF) shall assist the other agency by obtaining and providing the required security documents.

2.12.4. When access to RD or FRD outside the scope of aeronautical and space activities is required in the performance of NASA duties, a request for either a DOE or an NRC clearance shall be initiated by the CCS, who shall forward the necessary documents to the NASA CAF for appropriate action.

2.13 Guiding Principles for Adjudication, Suspension, Denial, or Revocation of Personnel Security Clearances

2.13.1. The Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Appendix B) serve as a guide for investigators and adjudicators to identify potential issues that may adversely affect an individual's eligibility for access to classified information.

2.13.2. Only the AA/OSPP or designee shall deny or revoke a security clearance.

2.13.3. The AA/OSPP, DSMD, and CCS may grant interim and final clearances or suspend security clearances, as appropriate.

2.13.4. Each adjudication shall be fully documented and recorded in the subject's security file and the Central Adjudication Activity (NASA CAF) personnel security database.

2.13.5. Information developed during the investigation process for a security clearance shall not be shared with the Center HRO or management while the investigation is pending. The DSMD or CCS may override this principle, if in their judgment the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals or is a threat to a critical mission or that the subject shall otherwise be ineligible for or lose continuation of Federal employment.

2.13.6. All reasonable efforts shall be pursued to fully develop potential issue information, as well as potentially favorable or mitigating information.

2.13.7. The CCS shall propose denials and revocations of security clearances to the NASA CAF. The AA/OSPP shall make final denial or revocation determinations after

consultation with the NASA CAF and the OGC, and as provided for under paragraph 2.15.4 of this NPR.

2.13.8. Requests for a security clearance (NASA Form 1630) shall result in an adjudicative determination unless, unrelated to any potential adjudication factor, the need for the security clearance no longer exists, such as severance of the subject's employment.

2.13.9. Subjects of adjudication must be allowed to review and refute any information developed during the investigation process that may make him or her ineligible for access to classified information, unless release of that information jeopardizes national security.

2.13.10. In the event of a denial or revocation of a security clearance, the subject is entitled to obtain review of the decision as prescribed in Section 5.2 of EO 12968.

2.13.11. The AA/OSPP, Center Director, CCS, or the DSMD may suspend a security clearance for cause.

2.13.12. The Center HRO, in coordination with the Security Office and supervisors, shall make employment suitability determinations under EO 10450 and other regulations. The Center HRO shall coordinate and document those determinations. They are separate and distinct from security clearance adjudications (see section 5.2(f) of EO 12968). See chapter 3 for requirements regarding employment suitability.

2.13.13. The policies and the procedures for the suspension, denial and revocation of a security clearance must not be confused with the procedures for the removal of an employee on national security grounds as set forth in Title 5, Chapter 75, Section 7532 of the U.S. Code. A CCS may pursue the removal of an employee on national security grounds under Section 7532, regardless of the sensitivity of the employee's position or whether the employee has access to classified information.

2.14 Adjudication of Personnel Security Clearance Status

2.14.1. The AA/OSPP, or designee, is empowered to deny or revoke an employee's security clearance.

2.14.2. Each investigation required for a specific clearance level must be complete with sufficient scope in order to appropriately adjudicate for access to classified information.

2.14.3. In instances when management, for reasons unrelated to the adjudicative process, withdraws a request for a security clearance and the subject of the investigation continues his or her employment with NASA, potential issue information developed during the investigative process must be documented in the employee's security file and suitability determinations made under the continuous evaluation program. The Center HRO and supervisory personnel, with the advice of the Security Office, shall make all suitability determinations under the continuous evaluation program. Refer to chapter 3, section 3.11, for requirements on processing suitability issues.

2.14.3.1. In cases where sufficient investigative information may not exist to complete the adjudication for a security clearance, the subject of an incomplete investigation must be apprised of any adjudicative issue information in accordance with E.O. 10450 and afforded an opportunity to comment on that information related to suitability for continued employment.

2.14.3.2. Explanations or mitigating information provided by the subject must also be documented in his or her security file.

2.14.4. Upon completion of an investigation that develops potential adjudicative issues, a personal interview of the subject shall be conducted by the appropriate security official.

2.14.4.1. During this interview the subject shall be advised of any issues and provided an opportunity to present relevant information to refute or mitigate the issues.

2.14.4.2. In isolated instances, when a personal interview is not practical, a written interrogatory shall be sent by the NASA CAF to the subject or the CCS shall be tasked to coordinate the reply.

2.14.4.3. The subject may be accompanied during the interview by counsel or other representative. All costs associated with such representation are at the subject's expense.

2.14.4.4. At the onset of a subject interview, the subject must be advised of the provisions of the Privacy Act of 1974 (5 U.S.C. 552a).

2.14.5. The initial adjudication will be made once the adjudicator has gathered all available pertinent information.

2.14.6. The Senior Adjudicator shall review the initial adjudication for fairness, completion, and proper application of the adjudication guidelines.

2.15 Denial or Revocation of Personnel Security Clearances

2.15.1. In the event of an unfavorable adjudication action, the NASA Central Adjudication Facility (NASA CAF) shall forward a documented proposal to deny or revoke a clearance to the AA/OSPP.

2.15.2. The AA/OSPP shall do one of the following after reviewing the file and the recommendation of the NASA CAF:

2.15.2.1. Remand the case to the NASA CAF for further work; or

2.15.2.2. Make a favorable adjudication of the information; or

2.15.2.3. In consultation with the Office of General Counsel, provide written notice to the subject of the denial or the revocation of the security clearance.

2.15.3. If the employee subsequently requests a review of the proposed action, or the subject provides new information for consideration, or both, the NASA CAF shall review the case, taking into consideration any new information provided. If no review is requested, or if the NASA CAF continues to recommend denial or revocation, after the review is conducted, the complete case file and the NASA CAF recommendation shall be forwarded to the AA/OSPP for action.

2.15.4. Actions of the AA/OSPP shall be conducted in accordance with the elements of section 5.2 (a) of EO 12968 and shall ensure that the rights of the subject are protected and due process is accorded, including the opportunity for the subject to appear in person to present relevant documents, materials, and information prior to the AA/OSPP' final determination. If the employee takes advantage of the opportunity to appear personally before the AA/OSPP, the AA/OSPP shall document such appearance by

means of a written summary or recording which shall be made a part of the subject's security record.

2.15.5. If the AA/OSPP provides notice of denial or revocation and the subject subsequently requests an appeal by a Security Adjudication Review Panel (SARP), the Administrator shall appoint that body. The panel shall be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members must have been the subjects of a favorable SSBI, and only one of the panel members shall be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the SARP or they may chose to appeal in person to the SARP. Any personal appearance before the SARP shall be documented by means of a written summary or recording which shall not be made a part of the subject's security record.

2.15.6. Prior to finalizing the SARP determination, a SARP panel member or the AA/OSPP may refer the SARP proposed decision to the Administrator for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If there is a referral to the Administrator, the Administrator's decision is final.

2.15.7. Upon determination that a clearance revocation or denial has been upheld, the case then becomes one of employment suitability and shall be referred to HRO for suitability determination per chapter 3, section 3.10.

2.16 Suspension of Personnel Security Clearances

2.16.1. The AA/OSPP, DSMD, Center Director, or the CCS shall suspend an individual's security clearance when information is developed that suggests the individual's continued access to classified information is not in the interest of national security.

2.16.1.1. Normally, an individual subject to a suspension action is advised of the suspension. However, there shall be instances when the suspending authority, working with management and the NASA Director, Security Management Division, and Director, Safeguards Division shall terminate an individual's access to new classified information, without the individual's knowledge, in order to preserve the integrity of an investigation.

2.16.1.2. The reason or reasons for a suspension need not be provided to the subject of a suspension.

2.16.1.3. Suspension of a security clearance shall not be open-ended. Every effort must be expended to complete the investigation and to adjudicate as soon as practical. All suspension actions must be resolved as soon as practical from the date of the suspension.

2.16.1.4. Suspension of an individual's access to classified information is not an adverse action. Suspension merely allows the agency time to investigate and adjudicate new information that may affect the individual's eligibility for access to classified information.

2.16.1.5. As a result of the temporary status of a suspension, the subject of a suspension is not entitled to the review procedures required for denial or revocation of a security clearance.

2.16.1.6. All suspensions enacted by Center Security Offices must be coordinated with the NASA CAF.

2.17 Continuous Evaluation of Personnel Security Clearance Eligibility

2.17.1. A personnel security clearance determination is based on a continuous assessment of an employee's personal and professional history demonstrating loyalty to the United States, strength of character, trustworthiness, reliability, discretion and sound judgment, as well as freedom from conflicting allegiances and potential coercion and willingness to abide by regulations governing the use, handling, and protection of CNSI.

2.17.2. In order to ensure that all persons who have been granted a security clearance remain eligible, all U.S. Government clearance holders shall be subject to a continuous evaluation of their qualification to meet the high standards of conduct expected of persons in national security positions.

2.17.3. Persons subject to a prior favorable personnel security determination who demonstrate behavior that places doubt on their loyalty, reliability, or trustworthiness or otherwise disqualifies that individual for continued eligibility for a security clearance shall be subject to further scrutiny and possible suspension of access to CNSI.

2.17.4. Center Directors and the CCS shall ensure a program of continuous evaluation for security clearance eligibility is developed that relies on all levels of management and all security clearance holders to be aware of the standards of conduct for qualification to hold a security clearance and their responsibility to report adverse behavior that shall be disqualifying. Where employees have significant involvement with handling, storing, marking CNSO, or exercising original or derivative classification, supervisors must include these responsibilities as a critical element of the employees' annual performance communication system documentation.

2.17.5. Supervisors and managers are critical to the success of the evaluation of the security clearance eligibility program. Supervisors shall report incidents of potentially disqualifying behavior that they are aware of to the CCS and be observant to potential changes in behavior of their subordinates that could cause potential risk to the national security information to which the employee has been entrusted.

2.17.6. Holders of security clearances and other employees with knowledge that an employee holds a security clearance shall be advised and periodically reminded to report to their supervisor or appropriate security officials when they become involved in behavior or become aware of such behavior of another cleared individual that could impact their continued eligibility for access to CNSI. A security clearance holder who fails to report disqualifying conduct involving other cleared personnel is also subject to suspension of access to CNSI, pending a security inquiry.

2.17.7. Personnel holding a Security Clearance are subject to random drug testing.

2.17.8. All reports of behavior that may impact continued eligibility to hold a security clearance shall be forwarded by the CCS to the NASA CAF, as appropriate.

2.18. CLASSIFIED VISITS AND MEETINGS

2.18.1. Classified Visits to Other Agencies . An employee who has a need to certify his/her security clearance for a visit to an agency or facility must initiate the appropriate visit form, letter, or telephonic action with the respective Center Personnel Security

Office or Special Security Officer.

2.18.1.1. The request shall be signed by the Center Personnel Security Officer or designated representative, the Special Security Officer, or member of the Security Management Division.

2.18.1.2. Completed Visit Requests will be faxed, mailed, or e-mailed, by the Center Security Office, to the appropriate external Agency Security Office for processing.

2.18.1.3. Visit requests should be for no more than one-year at time. Visit requests for longer than one-year are at the discretion of the visiting agency.

2.18.1.4. Only those clearances granted by the Security Management Division and contained in the automated listing of the Clearance Verification System may be certified.

2.18.2. Classified Visit Requests From Other Agencies and Classified Meetings. Employees hosting meetings involving classified information will advise the prospective attendees to have their security officers prepare and transmit certifications of the attendees' security clearances to the respective center personnel security office, Security Management Division, or the Special Security Officer. The certifications should include the investigation record information used as a basis to grant the clearance, Center POC point of contact, and purpose and duration of the visit request.

2.18.3. Special Access Program Visits . All visit requests involving a special access program shall be processed by the appropriate Special Security Officer.

2.19 Recordkeeping

2.19.1. Center Security Offices shall create and securely maintain personnel security investigative and screening records on all NASA civil service and contractor personnel security cases.

2.19.1.1. Files shall be maintained for a minimum of two (2) years after the individual's employment or access to NASA facilities or IT systems is terminated.

2.19.1.2. Files shall include the original forms submitted to initiate the investigation and screening, a summary of the results of any investigative and screening activity, a record of the final decision, and any subsequent actions.

2.19.1.3. Security offices shall safeguard these files pursuant to NPD 1440.6G, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules.

2.19.2. Subjects of personnel security investigations and screenings may request copies of excerpts, summaries, or any analytical extract of information from the NASA case file under the Freedom of Information and Privacy Act procedures. The subject may not be provided a copy of any third party investigations (i.e., OPM, DSS, FBI). The subject must obtain copies of the third party investigation directly from the appropriate agency.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov